Lecture 6.

Vector spaces over arbitrary fields.

We will have to review the Vector spaces part of your Linear Algebra course because now we are interested in vector spaces over arbitrary fields (not only real and complex numbers), especially over fields $\mathbb{Z}(p)$.

Let F be a field. Let $(V,+)$ be an abelian group. Let $F\times V$ be the Cartesian product of the sets F, V and let

$$F\times V \to V$$

be a mapping. In other words for every $\alpha\in F$, $v\in V$ we assign their "product" $\alpha v\in V$. We assume the following axioms:

- $\alpha(\beta v) = (\alpha\beta)v \quad \forall \alpha, \beta \in F,\ v \in V$
- $\alpha(v \pm w) = \alpha v \pm \alpha w \quad \forall \alpha \in F;\ v, w \in V.$

In other words, if we fix $\alpha \in F$ then the mapping $v \to \alpha v$, $V \to V$, is a homomorphism of the abelian group V into itself

- $(\alpha \pm \beta) v = \alpha v \pm \beta v \quad \forall \alpha, \beta \in F;\ v \in V$
- $1 v = v \quad \forall v$; here 1 is the identity element of the field F.

<u>Example</u>. $V = F^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in F\}$ the set of n-tuples.

$$\alpha(\alpha_1, \dots, \alpha_n) = (\alpha\alpha_1, \dots, \alpha\alpha_n).$$

Subspaces.

It is easy to see that for an arbitrary element $v \in V$

$$0 \cdot v = \mathbf{0}$$

where 0 is the zero element of the field F;
$\mathbf{0}$ is the zero element of the abelian group V.
For an arbitrary $\alpha \in F$

$$\alpha \cdot \mathbf{0} = \mathbf{0}.$$

We refer to elements from F as scalars.

<u>Subspaces.</u>

<u>Def.</u> A subset $W \subset V$ is called a <u>subspace</u> if 1) W is a subgroup of the abelian group $(V, +)$. In other words $\forall\, w_1, w_2 \in W$ we have $w_1 \pm w_2 \in W$;

2) $\forall$ scalar $\alpha \in F$, $\forall\, w \in W$ we have $\alpha w \in W$.

A subspace W can be viewed as a vector space on its own.

Example. Let $V = F^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in F\}$.
Let $W = \{(0, \alpha_2, \dots, \alpha_n) \mid \alpha_2, \dots, \alpha_n \in F\}$. Then W is a subspace of V.

If V is a vector space over a field F and we fix $\alpha \in F$ then $V \to V$, $v \to \alpha v$, is a unary operation. Therefore we could say that a vector space is a set with one binary operation $+$ and a family of unary operations $\alpha \cdot$, $\alpha \in F$.

Homomorphisms.

Let V, V' be vector spaces over the same field F.
A mapping $\varphi: V \to V'$ is a homomorphism of vector spaces (or a linear transformation) if 1) φ is a homomorphism of abelian groups $(V,+) \to (V',+)$,

2) $\varphi(\alpha v) = \alpha \varphi(v) \quad \forall \alpha \in F, v \in V.$

In other words φ preserves all operations: binary and unary.

A homomorphism is called an <u>isomorphism</u> if it is a bijection.

<u>Example.</u> $V = \{(\alpha_1, \dots, \alpha_n) / \alpha_i \in F\}$ rows;

$V' = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \alpha_i \in F \right\}$ columns.

$$\varphi((\alpha_1, \dots, \alpha_n)) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

<u>Span.</u>

Let V be a vector space / field F. Let $v_1, \dots, v_n \in V$. A vector $v = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n$; $\alpha_i \in F$, is called a <u>linear</u> combination of the vectors $v_1, \dots, v_n$.

A linear combination is said to be <u>nontrivial</u> if the coefficients $\alpha_1, \dots, \alpha_n$ are not all equal to 0.

The set

$$\mathrm{Span}(v_1, \dots, v_n) = \{\alpha_1 v_1 + \dots + \alpha_n v_n \mid \alpha_i \in F\}$$

of all linear combinations of $v_1, \dots, v_n$ is called the <u>span</u> of the vectors $v_1, \dots, v_n$.

The $\mathrm{span}(v_1, \dots, v_n)$ is always a subspace of V

<u>Example</u>. Let $V = \mathbb{R}^3$, $F = \mathbb{R}$; $v_1, v_2 \in V$ ~~Span(v_1, v_2)~~ are vectors that are not collinear. Then $\mathrm{span}(v_1, v_2)$

= the plane that contains the vectors v_1, v_2.

What is $\mathrm{span}(v)$? If $v \neq 0$ then $\mathrm{span}(v)$ is a line that contains v.

Linear independence.

Def. Let V be a vector space over a field F. A collection of vectors $v_1, \dots, v_n \in V$ is called linearly dependent if there exist coefficients $\alpha_1, \dots, \alpha_n \in F$, not all equal to zero, such that $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

Def. A collection of vectors $v_1, \dots, v_n \in V$ that is not linearly dependent is called linearly independent.

Lemma. Vectors $v_1, \dots, v_n \in V$ are linearly dependent if and only if one of these vectors is equal to a linear combination of other vectors.

Proof. If $v_i = \alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n$, then $\alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} - v_i + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n = 0$. Here one coefficient (at v_i) is equal to -1, so it is $\neq 0$.

Now suppose that $v_1, \dots, v_n$ are linearly dependent. Then there exists a linear combination $\alpha_1 v_1 + \dots + \alpha_n v_n$ such that not all α_i are $= 0$ and $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Let $\alpha_i \neq 0$. Move all other summonds to the right hand side and divide by α_i:

$$v_i = -\frac{\alpha_1}{\alpha_i} v_1 - \dots - \frac{\alpha_{i-1}}{\alpha_i} v_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} v_{i+1} - \dots - \frac{\alpha_n}{\alpha_i} v_n,$$

so v_i is equal to a linear combination of $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$. $\top$

<u>Example</u>. Let $V = \mathbb{R}^3$. Three vectors are linearly dependent if and only if they lie on

the same plane.

<u>Def.</u> A collection of vectors $v_1, \dots v_n \in V$ is called a <u>basis</u> (or a <u>base</u>) of

1) $v_1, \dots, v_n$ are linearly independent,

2) $V = Span(v_1, \dots, v_n)$.

<u>Proposition.</u> $\{v_1, \dots, v_n\}$ is a base if and only if an arbitrary element v from V can be expressed as a linear combination $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ <u>uniquely</u>.

<u>Proof.</u> Suppose that $\{v_1, \dots, v_n\}$ is a base. By the condition 2) an arbitrary element $v \in V$ can be represented as a linear combination of vectors $v_1, \dots, v_n$. Let us show that this presentation is unique.

Let $v = \alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n$,

where $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in F$. Then

$(\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \dots + (\alpha_n - \beta_n) v_n = 0$.

Since the collection $v_1, \dots, v_n$ is linearly indgrendent it follows that $\alpha_1 - \beta_1 = \dots = \alpha_n - \beta_n = 0$. The uniqueness is proved.

Now suppose that an arbitrary element $v \in V$ can be represented as a linear combination of $v_1, \dots, v_n$ uniquely. Then $V = \mathrm{Span}(v_1, \dots, v_n)$, so the 2d condition is satisfied. Lets prove that $v_1, \dots, v_n$ is linearly indgrendent. Suppose that $\alpha_1 v_1 + \dots + \alpha_n v_n = \mathbf{0}$, not all coefficients α_i are $= 0$. On the other hand we have $0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n = \mathbf{0}$. Now the zero vector has two different presentations, a contradiction. ⊥

<u>Proposition</u>. Suppose that $v_1, .., v_n \in V$ and $\mathrm{Span}(v_1, \ldots, v_n) = V$. Then some subset $v_{i_1}, \ldots, v_{i_d}$ of $v_1, \ldots, v_n$; $1 \le i_1 < .. < i_d \le n$; is a basis of V.

<u>Proof</u>. ~~Let~~ choose a subset $v_{i_1}, \ldots, v_{i_d}$ that is linearly independent and d is maximal with this property.

We will prove that $v_{i_1}, .., v_{i_d}$ is a basis of V. We already know that $v_{i_1}, .., v_{i_d}$ are linearly independent. It remains to show that $\mathrm{Span}(v_{i_1}, .., v_{i_d}) = V$, in other words, every element in a linear combination of $v_{i_1}, \dots, v_{i_d}$.

It is sufficient to show that every vector v_k, $1 \le k \le n$, is a linear combination of $v_{i_1}, \dots, v_{i_d}$. Indeed, suppose that

$$v_k = \alpha_{k1} v_{i_1} + \dots + \alpha_{kd} v_{i_d}, \quad \alpha_{kj} \in F,$$

$1 \le k \le n$.

An arbitrary element $v \in V$ is a linear combination of $v_1, \dots, v_d$:

$$v = \beta_1 v_1 + \dots + \beta_n v_n = \beta_1 (\alpha_{11} v_{i_1} + \dots + \alpha_{1d} v_{i_d}) +$$

$$\dots + \beta_n (\alpha_{n1} v_{i_1} + \dots + \alpha_{nd} v_{i_d}) =$$

$$(\beta_1 \alpha_{11} + \dots + \beta_n \alpha_{n1}) v_{i_1} + \dots + (\beta_1 \alpha_{1d} + \dots + \beta_n \alpha_{nd}) v_{i_d}$$

Hence an arbitrary element $v \in V$ is a linear combination of $v_{i_1}, \dots, v_{i_d}$.

Now, choose a vector v_k, $1 \le k \le n$.

If $k \in \{i_1, \dots, i_d\}$ then v_k is one of $v_{i_1}, \dots, v_{i_d}$, hence a linear combination of $v_{i_1}, \dots, v_{i_d}$.

Suppose that $k \notin \{i_1, \dots, i_d\}$. Then the collection of vectors $v_k, v_{i_1}, \dots, v_{i_d}$ is linearly dependent (since d is maximal!). There exist coefficients $\alpha, \alpha_1, \dots, \alpha_d \in F$, not all equal to 0, such that

$$\alpha v_k + \alpha_1 v_{i_1} + \dots + \alpha_d v_{i_d} = 0.$$

We claim that $\alpha \neq 0$. If $\alpha = 0$ then

$$\alpha_1 v_{i_1} + \dots + \alpha_d v_{i_d} = 0$$

and at least one of the coefficients α_i is $\neq 0$. But that would mean that $v_{i_1}, \dots, v_{i_d}$ are linearly dependent, a contradiction.

Hence $\alpha \neq 0$,

$$v_k = -\frac{\alpha_1}{\alpha} v_{i_1} - \dots - \frac{\alpha_d}{\alpha} v_{i_d}. \qquad \mathrm{I}$$

The following theorem was proved in the Linear Algebra course for vector spaces over $\mathbb{R}$. But specific properties of $\mathbb{R}$ were never used: the same proof works for vector spaces over an arbitrary field.

Theorem. Let V be a vector space over a field F. Let $v_1, \dots, v_n$ and $v_1', \dots, v_m'$ be bases of V. Then $n = m$.

So, all bases contain the same number of elements. This number is called the dimension of the vector space V.

Example. The space $V = F^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in F\}$ Has dimension n.

Indeed, let $e_i = (0, 0, \dots, \underset{i}{1}, 0, \dots, 0)$, $1 \le i \le n$, Then $e_1, e_2, \dots, e_n$ is a base of V.

<u>Proposition</u>. Let $F = \mathbb{Z}(p)$ and let V be an n-dimensional vector space over F. Then $|V| = p^n$.

<u>Proof</u>. Let $e_1, \dots, e$ ~~An arbitrary~~ Let $v_1, \dots, v_n$ be a base of V. An arbitrary element $v \in V$ can be uniquely represented as

$$v = \alpha_1 v_1 + \dots + \alpha_n v_n; \quad \alpha_1, \dots, \alpha_n \in F.$$

There are p candidates for α_1, p candidates for α_2, etc. Hence the number of such elements v is p^n. $\perp$